GUIA LGPD CREMESP

COMENTADO EDIÇÃO 2023

CREMESP
CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO

GUIA LGPD CREMESP COMENTADO EDIÇÃO 2023

EXPEDIENTE

Publicação do Conselho Regional de Medicina do Estado de São Paulo
Rua Frei Caneca, 1.282 – São Paulo – SP - CEP 01301-910
Tel. (11) 4349-9900 - www.cremesp.org.br

PRESIDENTE DO CREMESP

Irene Abramovich

COORDENADOR DA ASSESSORIA DE COMUNICAÇÃO

Wagmar Barbosa de Souza

CHEFE DA ASSESSORIA DE COMUNICAÇÃO

Marcos Michelini

GERÊNCIA DA PROCURADORIA JURÍDICA AUTÁRQUICA

Carlos Magno dos Reis Michaelis Júnior

ENCARREGADO DE PROTEÇÃO DE DADOS

Elcio Lima Garcia

IDEALIZAÇÃO

Angelo Vattimo, Flavia Amado Bassanezi
e Joaquim Francisco Almeida Claro

ELABORAÇÃO

Comissão de Gestão de Segurança da Informação
e Proteção de Dados Pessoais do Cremesp
Conselheiros: Angelo Vattimo (coordenador), Irene Abramovich, Joaquim Francisco Almeida Claro, Maria Camila Lunardi e Wagmar Barbosa de Souza.
Integrantes: Carlos Magno dos Reis Michaelis Júnior, Cristina Aparecida Calabrese, Cynthia Aparecida dos Santos Silva, Djalma Gomes Rodrigues, Elcio Lima Garcia, Erika Ura Kusano, Elmo Menezes de Couto, João Carlos Ferreira Júnior, Julia Naddaf Remer, Luis Gonzaga Amim, Marcelo Gonçalves de Castro, Marcos David, Marcos Michelini, Paula Véspoli Godoy, Silmar Vizcaino e Suzana Dantas dos Santos.

REVISÃO

Aglaé Silvestre, Concília Ortona, Fátima Barbosa, Ivolethe Duarte, Julia Naddaf Remer, Marcos Michelini e Nara Damante

DIAGRAMAÇÃO E CAPA

Alexandre Paes Dias

CAT – Central de Atendimento Telefônico
Tel. (11) 4349-9900
Atendimento na sede: Rua Frei Caneca, 1.282 (das 9h às 18 horas)
E-mail: lgpd@cremesp.org.br

ÍNDICE

INTRODUÇÃO

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

O Conselho Regional de Medicina do Estado de São Paulo (Cremesp), ciente da nova regulamentação referente à Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº13.709/2018 – elaborou este guia de orientação aos profissionais médicos sobre a nova legislação, suas exigências e adequações a serem implementadas em seu cotidiano de trabalho. O estudo, efetivado pela Comissão de Gestão de Segurança da Informação e Proteção de Dados Pessoais do Conselho, é notadamente voltado para consultórios médicos de pequeno porte, os quais representam grande número das pessoas jurídicas registradas no Cremesp.

É patente que as instituições públicas e privadas de saúde de maior porte necessitam se adequar à nova norma e, certamente, já estão estabelecendo suas próprias políticas internas e fluxos de proteção de dados pessoais, os quais deverão ser respeitados por toda equipe de saúde. Situação distinta é a do médico que em seu consultório é o controlador de dados pessoais e sensíveis de seus pacientes e colaboradores, que deverá se conscientizar e se organizar sob uma nova perspectiva de proteção de dados pessoais. Este guia tem como intento auxiliá-lo neste processo.

O sigilo e a confidencialidade das informações dos pacientes e usuários do sistema de saúde já são de conhecimento dos profissionais que atuam na área, em especial, dos médicos, para os quais o sigilo é princípio deontológico basilar da profissão, pilar da relação médico-paciente, como previsto no Código de Ética Médica.

O conjunto de regulamentações já existentes na área da saúde foi ampliado, em 2018, com a promulgação da LGPD, a qual foi publicada para proteger o direito fundamental de privacidade, garantido na Constituição Federal em seu artigo 5º, inciso X, como direito da personalidade,

da integridade moral e da dignidade de cada ser humano. Assim, além das regulamentações já conhecidas pelos médicos, oriundas da Agência Nacional de Saúde (ANS), da Agência Nacional de Vigilância Sanitária (Anvisa), do Conselho Nacional de Saúde (CNS) e do Conselho Federal de Medicina (CFM), dentre outros órgãos de controle, há esta nova normativa, que veio regulamentar o tratamento de dados pessoais dos indivíduos, estejam eles dispostos em meio físico ou digital.

A norma exige implementação de novos procedimentos e fluxos de segurança no tratamento de dados pessoais, trazendo conceitos e obrigações referentes à proteção de dados pessoais dos titulares. Daí a importância de consultórios médicos se adequarem à lei e implantarem ações e procedimentos internos que garantam o tratamento de dados pessoais de forma apropriada. Essas medidas visam respeitar os princípios trazidos pela LGPD, mantendo a confidencialidade dos documentos do paciente — principalmente seus prontuários médicos — garantindo que eles sejam armazenados de forma segura (física ou digital) e acessados somente pelos profissionais que de fato necessitem ter conhecimento das informações clínicas do paciente.

Importante considerar que os dados pessoais aos quais os médicos têm acesso são dados sensíveis, conforme classificação da LGPD. Também não se pode olvidar que, nos consultórios, existem dados pessoais de outras pessoas, os quais podemos elencar como: colaboradores/funcionários, prestadores de serviço e demais fornecedores, que deverão ser adequadamente tratados.

Este guia tem o propósito de orientar de maneira sucinta como o médico, em seu cotidiano deverá se adequar às obrigações estabelecidas na LGPD visando, além da boa prática médica, à governança na proteção dos dados pessoais de todos os envolvidos neste ambiente.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

I - PARA ENTENDER A LGPD

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

DEFINIÇÕES

A Lei Geral de Proteção de Dados (LGPD) dispõe sobre o tratamento e a proteção de dados pessoais, sejam eles em meios físicos ou digitais, com o objetivo de proteger os direitos fundamentais da liberdade e da privacidade. Essa norma trouxe grande impacto às pessoas físicas e organizações, no que tange ao tratamento de dados pessoais e dados pessoais sensíveis.

DADOS PESSOAIS

São as informações relacionadas à pessoa natural que permitem identificá-la, como por exemplo, nome, RG, CPF, CRM, CNH, email, celular e endereço residencial, entre outros dados.

DADOS PESSOAIS SENSÍVEIS

Informações que se referem à origem racial ou étnica, religião, orientação sexual, posicionamento político, filiação a sindicato ou outras organizações, condições de saúde, dados genéticos ou biométricos são considerados dados pessoais sensíveis. Esses elementos devem ser tratados de maneira mais criteriosa e, por isso, exigem maior nível de segurança, para que seja evitada utilização com fim inadequado. A área da Saúde é uma das mais afetadas por essa definição, uma vez que esse

conjunto de informações não deve ser tratado com fins discriminatórios ou preconceituosos, pois referem-se a doenças, relatórios médicos, prontuários, resultados de exames, dados biométricos, dentre outros dados específicos do paciente.

TRATAMENTO DE DADOS PESSOAIS

O artigo 5, inciso X, da LGPD, estabelece que toda operação realizada com dado pessoal é tratamento de dados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim, em consultórios médicos, desde a coleta dos dados do paciente para simples cadastro até o armazenamento de seu prontuário médico (físico ou digital), transmissão de dados e compartilhamento com hospitais, laboratórios e operadoras, são formas de tratamento de dados pessoais, uma vez que tratam de informações sensíveis desses pacientes.

DADOS ANONIMIZADOS E PSEUDONIMIZADOS

A anonimização é a utilização de meios técnicos de tratamento que faz com que um dado perca a possibilidade de associação, direta ou indireta, a um indivíduo.

A pseudonimização é um procedimento de anonimização em que um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, ao ser substituído por um identificador artificial ou pseudônimo.

Segundo o Serpro[1]: *"Se um dado for anonimizado, então a LGPD não se aplicará a ele. Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.*

OS ENVOLVIDOS

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Exemplos de titulares de dados pessoais em consultórios médicos são os pacientes, seus familiares/visitantes, prestadores de serviços, funcionários e colaboradores.

Agentes de tratamento: são o controlador e o operador. Dentre as obrigações dos agentes de tratamento, destacam-se a obrigatoriedade de adoção de medidas de segurança, técnicas e administrativas, para proteção de acessos não autorizados; o registro das operações de tratamento de dados, e a elaboração de relatório de impacto.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Exemplos de controladores são os próprios consultórios médicos e os médicos responsáveis pelo paciente.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Exemplos de operadores: secretárias dos mé-

[1] https://shre.ink/kdEI

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

dicos, prestadores de serviços de Tecnologia da Informação, colaboradores da área administrativa do consultório médico, contador e departamento pessoal.

Encarregado: pessoa indicada, pelo controlador e pelo operador, para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Autoridade Nacional de Proteção de Dados (ANPD[2]): é o órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para sua implementação. Foi criada em 13 de junho de 2022, por medida provisória, e transformada em Autarquia de natureza especial, tendo como principais funções promover o conhecimento das normas sobre proteção de dados pessoais, além de fiscalizar e aplicar sanções, em caso de descumprimento da legislação.

PRINCÍPIOS

Os princípios da Lei Geral de Proteção de Dados (LGPD) encontram-se em seu artigo 6°, prevendo a norma que qualquer tratamento de dados pessoais deverá observar a **boa-fé**, além de outros dez princípios:

1 - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; ou seja, tratamento de dados com aplicação clara, específica e válida.

[2] https://shre.ink/kdDY

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

2 - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. A adequação significa serem compatíveis às finalidades anteriormente descritas.

3 - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Quanto à necessidade, é a utilização somente da informação indispensável para atingir seu objetivo.

4 - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Estabelece que todo titular de dados pessoais tem o direito, de forma não onerosa, à consulta sobre o tratamento de suas informações.

5 - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Princípio que garante mais um direito do titular no que tange à condição de seus dados.

6 - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e seus respectivos agentes, observados os segredos comercial e industrial. Reiteradamente, mais um princípio que se refere ao direito do titular em obter esclarecimentos a respeito do tratamento e os agentes envolvidos.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

7 - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Visa priorizar o controle de acesso aos dados pessoais e, no caso do exercício da Medicina, o controle de dados sensíveis.

8 - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Estabelece a necessidade de regras para garantir a salvaguarda dos dados pessoais.

9 - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos, ou seja, a não utilização dos dados com fins distinguidores, por exemplo, com a finalidade de discriminar determinado paciente de um plano de saúde.

10 - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. Este princípio norteia o entendimento dos papéis dos agentes de tratamento de dados, inclusive no que diz respeito à responsabilidade.

Os princípios previstos na LGPD visam assegurar que o tratamento de dados será realizado com o mínimo necessário para atingir suas finalidades legítimas e específicas, de modo que o titular esteja ciente de como será realizado o tratamento (transparência) e de que seus dados estão sendo protegidos de acessos indevidos e de vazamentos.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

BASES LEGAIS

A LGPD elenca, em seu artigo 7°, as hipóteses de tratamento de dados pessoais que são, portanto, utilizados usualmente em consultórios e que devem se enquadrar em uma das bases legais estabelecidas no referido artigo. São dez as bases legais que permitem o tratamento de dados pessoais:

I. CONSENTIMENTO INFORMADO DO PACIENTE E DEMAIS PESSOAS QUE FAZEM PARTE DAS ATIVIDADES DO CONSULTÓRIO

O consentimento do titular é a manifestação livre, informada, inequívoca, pela qual o titular concorda com o tratamento para uma finalidade determinada. Deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. As autorizações genéricas para o tratamento de dados pessoais são consideradas nulas.

II. CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA PELO CONTROLADOR (PROFISSIONAL OU SERVIÇO DE SAÚDE)

Com essa base jurídica, o controlador pode tratar dados pessoais – sem consentimento – do titular para cumprir uma obrigação legal ou regulatória. O tratamento de dados, nesses casos, não é uma escolha discricionária do controlador, mas uma obrigação a se cumprir.

III. TRATAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA PARA EXECUÇÃO DE POLÍTICAS PÚBLICAS

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Conforme o Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público[3]: *"recomenda-se que o conceito de política pública seja interpretado de forma ampla, de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução". Por exemplo: política de controle do tabagismo, programas de vacinação, programa farmácia popular.*

IV. REALIZAÇÃO DE ESTUDOS POR ÓRGÃOS DE PESQUISA, GARANTIDA, SEMPRE QUE POSSÍVEL, A ANONIMIZAÇÃO DOS DADOS PESSOAIS

Os institutos de pesquisa são entidades da administração pública, direta ou indireta, ou ainda, pessoa jurídica de direito privado sem fins lucrativos, legalmente constituídos conforme as leis brasileiras, que tenham como objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico (Artigo 5º, XVIII).

V. EXECUÇÃO DE CONTRATO E PROCEDIMENTOS PRELIMINARES RELACIONADOS A CONTRATO DOS QUAIS SEJAM PARTE O TITULAR, A PEDIDO DO TITULAR DOS DADOS

Base legal para utilização de dados pessoais para fazer cumprir contratos, como de prestação de serviços ou contrato de trabalho. Considerando a área da saúde, podemos citar

[3] https://shre.ink/kdDd

contrato com os colaboradores ou contrato de prestação de serviços médicos/honorários com pacientes.

VI. EXERCÍCIO REGULAR DE DIREITO EM PROCESSO JUDICIAL, ADMINISTRATIVO OU ARBITRAL

O objetivo é resguardar o direito ao acesso à Justiça, seja no âmbito administrativo, arbitral ou judicial, não sendo necessário consentimento do titular para seu aproveitamento. Esta base legal pode ser aplicada quando for necessário o aproveitamento de dados pessoais dos pacientes para defesa do médico em processos judiciais e/ou administrativos.

> O Código de Ética Médica já prevê, em seu artigo 89, que cópias de prontuários sob sua guarda poderão ser utilizadas para atender ordem judicial ou para sua própria defesa, ressaltando que, neste último caso, deverá o médico solicitar que seja observado o sigilo profissional.

VII. PROTEÇÃO DA VIDA OU DA INCOLUMIDADE FÍSICA DO TITULAR OU DE TERCEIRO

Essa hipótese prevê o tratamento e, inclusive, o compartilhamento de dados pessoais em situações, quando necessário, para proteger a vida ou para a preservação da segurança de um indivíduo. No âmbito da Saúde, o uso de dado pessoal, como: tipo sanguíneo no atendimento de emergência, ou mesmo, dados pessoais contidos no seu documento de identificação, para que se estabeleça contato com familiares ou verificação de convênio médico.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Dessa forma, se o tratamento ocorrer para garantir a vida e a integridade física da pessoa, está amparado por lei.

VIII. TUTELA DA SAÚDE, EXCLUSIVAMENTE, EM PROCEDIMENTO REALIZADO POR PROFISSIONAIS DE SAÚDE, SERVIÇOS DE SAÚDE OU AUTORIDADE SANITÁRIA

Procedimentos realizados somente por profissional de saúde e/ou serviços de saúde permitem o tratamento de dados conforme base legal aqui descrita. É admitido o tratamento de dados para a tutela da saúde como, por exemplo, nos casos de intervenção cirúrgica.

IX - QUANDO NECESSÁRIO PARA ATENDER AOS INTERESSES LEGÍTIMOS DO CONTROLADOR OU DE TERCEIRO, EXCETO NO CASO DE PREVALECEREM DIREITOS E LIBERDADES FUNDAMENTAIS DO TITULAR QUE EXIJAM A PROTEÇÃO DOS DADOS PESSOAIS

É subjetivo o termo “legítimo interesse”, o que exige que sua aplicação seja realizada de maneira criteriosa, sendo necessário levar em conta o interesse do controlador e o direito do titular. O Artigo 10, §§ 2º e 3º, da LGPD, prevê que essa base legal deve ser documentada, pois a ANPD poderá solicitar ao controlador o relatório de impacto à proteção de dados baseados nessa hipótese legal.

X - PROTEÇÃO DO CRÉDITO, INCLUSIVE QUANTO AO DISPOSTO NA LEGISLAÇÃO PERTINENTE

Essa base legal tem por finalidade garantir que, em situação de cobrança de dívidas contraídas, possam ser consultadas as instituições de proteção de crédito reconhecidas pelo Código de Defesa do Consumidor como entidades de caráter público.

HIPÓTESES DE TRATAMENTO DE DADOS SENSÍVEIS

Pode ocorrer o tratamento de dados pessoais sensíveis somente em situações específicas pontuadas no artigo 11 da LGPD (abaixo). Ou seja, é inadmissível o tratamento de dados sensíveis sem consentimento ou além dessas possibilidades previstas. Vale ressaltar, ainda, que a **comunicação ou compartilhamento desses dados é proibida com o objetivo de obter vantagem econômica.**

> **"I. Quando o titular ou seu responsável legal consentir, para finalidades específicas;**

> **II. Sem fornecimento de consentimento titular, quando for indispensável para:**

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) Proteção da vida ou da incolumidade física do titular ou de terceiro;

f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrô-

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

nicos, resguardados os direitos mencionados no Artigo 9º desta lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.

§ 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do Artigo 23 desta lei.

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:

I - a portabilidade de dados quando solicitada pelo titular; ou

II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.

§ 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários."

Como se vê, os dados sensíveis – que incluem os da saúde do indivíduo – possuem regulação mais rigorosa e, por isso, sua finalidade deve ser delimitada e dada a devida ciência ao paciente sobre o motivo daquela informação estar sendo coletada.

CONSENTIMENTO

O conceito de consentimento é definido pelo artigo 5º da LGPD como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". É um dos requisitos para tratamento de dados, conforme descrito como base legal, e deverá ser realizado por escrito ou por outro meio que demonstre a manifestação de vontade do titular dos dados. O consentimento poderá ser revogado a qualquer momento com a manifestação expressa do titular de dados de maneira gratuita e facilitada.

O consentimento é tido como principal ferramenta para o tratamento de dados pessoais. Mas, na área da Saúde, é um documento que pode ser dispensado, dependendo da base legal utilizada para fundamentar o tratamento como, por exemplo, para a tutela da saúde nos casos de urgência e emergência em que o paciente não possui naquele momento condições de consentir e a intervenção deve ser imediata.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

II - TRATAMENTO DE DADOS EM CONSULTÓRIOS MÉDICOS

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

DIREITO DOS TITULARES

A coleta de dados pessoais é o primeiro passo na relação entre o paciente e o consultório médico. A Lei Geral de Proteção de Dados trouxe mais segurança ao tratamento dos dados sensíveis dos pacientes. A lei orienta aos médicos a forma em que será armazenado, compartilhado, arquivado e transmitido os dados pessoais e sensíveis, nos estabelecimentos de Saúde.

No cotidiano dos consultórios médicos, secretárias, atendentes, enfermagem e o próprio médico estão a todo tempo tratando e compartilhando dados pessoais dos pacientes, inclusive, via internet. Daí o cuidado que se deve ter com o vazamento dessas informações, uma vez que o paciente pode ser facilmente identificado e ter a sua intimidade violada.

O prontuário médico — documento que retrata toda a intimidade e saúde dos pacientes, conforme Resolução CFM 1821/2007, seja ele em papel ou eletrônico — deve ser adequado à segurança necessária, evitando-se a violação do sigilo nele contido.

Toda a equipe que tem acesso a ele precisa ser treinada e monitorada quanto aos procedimentos de segurança e riscos de vazamento de seu conteúdo.

As situações do dia a dia dos estabelecimentos de saúde que envolvem o tratamento de dados pessoais são: criação e armazenamento de prontuários médicos (físico ou virtual); transmissão de informações entre profissionais sobre o estado de saúde do paciente; e troca de informação entre o estabelecimento de saúde, operadoras de saúde e farmácias, entre outros.

Os titulares têm direito a acesso e correção de seus dados, portabilidade, informações de compartilhamento, revogação de consentimento e eliminação de seus dados.

LGPD NOS CONSULTÓRIOS

A LGPD possibilita que toda pessoa natural ou jurídica de direito público ou privado realize tratamento de dados pessoais: independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional; que a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

O consentimento do paciente deve ser uma manifestação livre, informada e inequívoca (consignada de forma escrita) pela qual ele concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Caberá ao estabelecimento de saúde comprovar que o consentimento foi obtido em conformidade com o disposto na LGPD. Por essa razão, o consultório deverá se valer de meios eficazes para obter e armazenar o consentimento de seus pacientes, consumidores, usuários ou colaboradores para o tratamento de dados pessoais.

MECANISMOS PARA OBTENÇÃO DE CONSENTIMENTO

- Elabore para o titular um documento com esclarecimentos objetivos acerca do tratamento de dados pessoais a ser efetuado. Esse documento não é tão diferente do Termo de Consentimento Livre e Esclarecido utilizado por muitos estabelecimentos de saúde, podendo este apenas ser adaptado para contemplar a finalidade do tratamento de dados pessoais;
- O consentimento deve referir-se a finalidades determinadas. Isso porque as autorizações genéricas para o tratamento de dados pessoais serão nulas, conforme a LGPD;
- Se o consentimento for fornecido por escrito em documento contendo outras cláusulas além dessa, a disposição que trata da anuência deve ser destacada.

Obtido o consentimento, outros cuidados ainda são necessários. Deve-se, por exemplo, viabilizar ao titular dos dados pessoais que revogue, a qualquer momento e gratuitamente, o consentimento anteriormente dado. Nesse caso, os estabelecimentos de saúde devem exigir a manifestação escrita e em termos expressos do titular solicitando a revogação.

Se o estabelecimento de saúde necessitar comunicar ou compartilhar com outros estabelecimentos ou pessoas os dados pessoais do titular que consentiu coleta e o armazenamento de certos dados, deve obter consentimento específico para essa finalidade.

DADOS PESSOAIS DE CRIANÇAS E ADOLESCENTES

O Estatuto da Criança e do Adolescente considera "crianças" indivíduos de 0 a 12 anos incompletos e como "adolescentes" indivíduos de 12 a 18 anos incompletos.

O tratamento de dados pessoais de crianças e de adolescentes, como estabelece o Artigo 14 da LGPD, deverá ser realizado sempre com o consentimento específico de um dos pais ou pelo responsável legal.

Conforme a **Cartilha para consultórios - Área da Saúde da OAB/SP[4]:**
"Os dados pessoais sensíveis mais delicados são os relacionados a adolescentes. A regra da LGPD deixou muitas questões em aberto e com alguns pontos de dúvida quando analisado o contexto legal geral. Assim, alguns pontos podem ajudar o profissional nessa decisão no caso específico: Os menores de 16 anos são absolutamente incapazes para atos da vida civil, sendo assim, a melhor conduta é providenciar o consentimento específico e destacado de um dos pais ou responsável; Havendo conflito entre os interesses de saúde do adolescente e adultos, o interesse na preservação da

[4] Cartilha_Consultorios_OABSP_ComPriv_GT_Priv_Saude_141221-1.pdf

saúde do adolescente deverá prevalecer, especialmente em relação aos relativamente incapazes (entre 16 e 18 anos).”

INVENTÁRIO DE DADOS PESSOAIS

Sob a ótica da Lei Geral de Proteção de Dados (LGPD), o inventário de dados pessoais em consultórios é um processo importante para garantir a privacidade e a segurança das informações dos pacientes. As etapas seguintes ajudam a elaborar um inventário eficaz:

1. Identificação dos dados pessoais: identifique todas as informações pessoais que são coletadas, armazenadas, processadas ou compartilhadas pelo consultório. Isso pode incluir informações como nome, endereço, data de nascimento, histórico médico e informações financeiras, entre outras.

2. Fonte dos dados: anote a fonte de cada item de informação pessoal. Por exemplo: se foi fornecida por paciente, coletada durante a consulta médica ou obtida de terceiros.

3. Finalidade da coleta de dados: anote a finalidade da coleta de cada item de informação pessoal. Por exemplo: a informação pode ser coletada para fins médicos, administrativos ou cobrança.

4. Armazenamento dos dados: identifique onde cada item de informação pessoal é armazenado, se é em papel, em arquivo digital ou em outro meio.

5. Compartilhamento de dados: anote com quem a informação pessoal é compartilhada. Por exemplo: com outros profissionais de saúde, empresas de cobrança ou órgãos regulatórios.

6. Prazos de retenção: anote os prazos de retenção para cada item de informação pessoal, de acordo com a legislação em vigor e as práticas internas do consultório.

7. Medidas de segurança: identifique as medidas de segurança implementadas para proteger a privacidade e a segurança das informações pessoais, incluindo medidas técnicas, administrativas e físicas.

Uma vez elaborado o inventário, é importante mantê-lo atualizado periodicamente e revisar suas políticas e práticas de privacidade e segurança de dados para garantir o cumprimento da LGPD.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

III - COMPARTILHAMENTO DE DADOS PESSOAIS

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

O uso compartilhado de dados é definido pelo inciso XVI, do artigo 5º da LGPD, como *"comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados"*.

É direito do titular obter informações de entidades públicas e privadas de como seus dados são compartilhados e para quais finalidades.

A comunicação ou compartilhamento de dados sensíveis inerentes à saúde, com o objetivo de obter qualquer tipo de vantagem econômica, seja de forma direta ou indireta, como para seleção de riscos na contratação e exclusão de beneficiários, é vedada pela LGPD. Ou seja, é proibida, por exemplo, a troca de informações entre farmácias e operadoras de saúde sobre os tipos de medicamentos que um titular faz uso antes de aceitá-lo como beneficiário (Artigo 11, § 5º).

A lei estabelece, no entanto, as seguintes exceções relativas a esta regra: a prestação de serviços da saúde, assistência farmacêutica e assistência à saúde.

As exceções estabelecidas devem ser utilizadas sempre atreladas ao interesse do titular, como em:

- Serviços auxiliares de diagnóstico e terapia;

e para:

- Realização de exames laboratoriais ou cumprimento de alguma prescrição de tratamento, desde que em benefício do titular dos dados pessoais;
- Em atendimento às necessidades dos prestadores de serviços e gestores do SUS;
- Fins de portabilidade de dados, quando consentido pelo titular, em atendimento ao direito de portabilidade dos dados previsto no Artigo 18, V, da LGPD;
- Transações financeiras e administrativas resultantes do uso e da prestação de serviços de saúde, como pedidos de reembolso por despesas médicas ou em situações nas quais a operadora de saúde só autoriza a realização de procedimentos médicos mediante o fornecimento de laudo de exames do titular dos dados.

COMPARTILHAMENTO DE DADOS PESSOAIS TRATADOS

Operadoras: Em se tratando de paciente que possui contrato com operadora de saúde, não é incomum que a contratada requeira relatório detalhado ou cópia do prontuário, comprovando a necessidade do pedido de exame ou procedimento cirúrgico, sob pena de glosa. O médico poderá fornecer os dados solicitados pelas operadoras se o paciente assim autorizar. Caso o paciente não autorize esse compartilhamento de dados, nos termos da Resolução CFM nº 1.614/2001, as operadoras poderão indicar auditor para acessar, *in loco*, toda a documentação necessária, sendo-lhe vedada a retirada dos prontuários ou

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

cópias da instituição. Se necessário, é permitido examinar o paciente, desde que devidamente autorizado pelo mesmo, quando possível, ou por seu representante legal. E, ainda, no caso de falecimento do paciente, vale a citação do artigo 77 do Código de Ética Médica, que proíbe ao médico prestar informações a seguradoras, além das contidas na Declaração de Óbito, salvo por expresso consentimento do seu responsável legal.

No que se refere à contratação de planos de saúde, é importante destacar que o artigo 11, §5º, da LGPD, veda às operadoras de saúde o tratamento de dados de saúde para prática de seleção de riscos na contratação e exclusão de beneficiários.

Médicos: É comum o compartilhamento de dados entre médicos, seja para obter uma segunda opinião, seja para discussão de casos. O artigo 73 do Código de Ética Médica diz que é vedado ao médico revelar fato que tenha conhecimento em virtude do exercício de sua profissão. Essa proibição é extensiva, conforme preconiza o artigo 54 do mesmo postulado ético, na relação entre médicos. O compartilhamento de dados é possível neste caso, desde que autorizado pelo paciente. O dono do segredo médico, bem como dos dados sensíveis, é o paciente, cabendo a este decidir sobre o pretenso compartilhamento com outro médico, além de seu médico assistente.

O médico é o controlador dos dados pessoais de seus pacientes. Portanto, deve trocar informações sempre por meio de plataformas seguras e adequadas.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Laboratórios: É costumeiro que, quando da realização de exames solicitados pelo médico assistente, o laboratório encaminhe não só ao paciente o exame acompanhado de seu laudo, como também ao médico assistente que o solicitou.

No entanto, nesse compartilhamento entre médico assistente e laboratório deve se resguardar o devido sigilo profissional e a proteção de dados, haja vista a existência de dados sensíveis do paciente.

Os laboratórios devem adequar seus fluxos para que, quando haja coleta dos dados, eles sejam tratados de maneira precisa para realização do diagnóstico e compartilhados somente com pessoas devidamente autorizadas pelo paciente.

Dever legal: A LGPD prevê, dentre as bases legais para tratamento de dados pessoais e sensíveis sem a devida autorização do titular/paciente, os casos de *"cumprimento de obrigação legal ou regulatória pelo controlador"*
O Código de Ética Médica já prevê, em seu artigo 73, que é vedado ao médico:
"Artigo 73 – Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.
Parágrafo único – Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha (nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento); c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal."

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Como exemplo de dever legal a ser cumprido pelo médico está a realização de notificação compulsória de doenças infecto-contagiosas (Lei nº 6.259/75) https://www.planalto.gov.br/ccivil_03/leis/l6259.htm. Também a suspeita de crimes, abusos de crianças, mulheres e idosos, desde que não exponha o seu paciente a procedimento criminal, como, por exemplo, o apontado pela Lei nº 10.778/2003, https://presrepublica.jusbrasil.com.br/legislacao/98170/lei-10778-03, que estabelece a notificação compulsória, no território nacional, do caso de violência contra a mulher que for atendida em serviços de saúde públicos ou privados.
Como se vê, a quebra do sigilo médico ocorre apenas quando as informações dizem respeito ao interesse coletivo, em situações que coloquem em risco terceiros ou a sociedade.

Familiares: Compete ao médico prestar todos os esclarecimentos clínicos e diagnósticos ao paciente. Contudo, deve-se observar com cautela a questão do compartilhamento desses dados do paciente com seus familiares, pois o dono do sigilo médico é o paciente, cabendo apenas a ele decidir sobre a sua revelação. Somente no caso de paciente que não responde pelos atos da vida civil é que a revelação dos dados obtidos no exercício da profissão pode ocorrer ao seu responsável legal, objetivando sempre a sua saúde e bem-estar.

O Conselho Federal de Medicina possui entendimento de que, no caso de paciente falecido, o prontuário médico poderá ser liberado somente para parentes em até 4º grau, desde que comprovado o vínculo familiar e a ordem de vocação hereditária.

Telemedicina: A Telemedicina está disciplinada atualmente na Resolução CFM nº 2.314/2022, a qual veio substituir a Resolução CFM nº 1.643/2002, considerando que este modelo existe para contribuir e favorecer o intercâmbio de informações entre médicos e entre médicos e pacientes, visando os melhores resultados ao paciente. Essa Resolução prevê que os dados coletados deverão ser preservados e armazenados sob a responsabilidade do médico (controlador), que deve seguir a LGPD quanto às finalidades dos dados tratados. A Telemedicina, por envolver transmissão de dados sensíveis, deverá ser realizada com cuidados técnicos e administrativos necessários para garantir a privacidade dos dados envolvidos.

IV - MEDIDAS E AÇÕES

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

ETAPAS

PLANEJAMENTO → IMPLANTAÇÃO → MONITORAMENTO

1 - PLANEJAMENTO

Entendimento de quais são as primeiras informações e dados pessoais coletados que devem ser conhecidos e tratados, segundo a LGPD:

Etapa	Atividade
1	Nomeação do encarregado;
2	Identificação das medidas de segurança do consultório, no âmbito físico e eletrônico, tais como alarme, travas nas janelas, portas e armários, bem como os acessos aos dados pessoais via sistemas e plataformas digitais;
3	Diagnóstico do estágio atual nas operações de tratamento de dados (inventário): quais dados devem ser tratados, necessidades, armazenamento, acessos, base legal e compartilhamentos;
4	Análise do sistema de segurança da informação;
5	Levantamento dos contratos que envolvam compartilhamento de dados pessoais.

2 - IMPLANTAÇÃO

Criação e operacionalização de mecanismos que protegem os direitos do indivíduo em relação à privacidade de seus dados pessoais, com destaque para:

Etapa	Atividade
1	Elaboração das normas e políticas internas para o tratamento dos dados pessoais;
2	Instituição da política de segurança da informação;
3	Limitação do acesso aos dados pessoais tratados por meio de perfis e senhas, bem como o espaço físico com restrição de acesso;
4	Treinamento e conscientização dos colaboradores e parceiros para tratamento e proteção de dados pessoais;
5	Disponibilização de canal de comunicação com os titulares (e-mail, sistema...);
6	Adoção de novas medidas de segurança, inclusive diretrizes e cultura interna;
7	Elaboração ou atualização de termos de consentimento;
8	Adequação das cláusulas contratuais de contratos que preveem o compartilhamento de dados pessoais;
9	Eliminação de documentos que estejam fora do prazo de armazenamento obrigatório.

3 - MONITORAMENTO

Acompanhamento contínuo do atendimento aos requisitos da LGPD, incluindo:

Etapa	Atividade
1	Revisão periódica do inventário;
2	Definição dos indicadores de segurança na proteção de dados;
3	Gestão de incidentes de vazamento, caso ocorram;
4	Análise de resultados e relatório de impacto.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

INTERAÇÕES

A proteção de dados é uma tarefa que deve envolver todos dentro da instituição de saúde. Para isso, as interações entre as pessoas e os setores da organização são importantes para a implantação da cultura e operacionalização da proteção de dados.

Jurídico – Colabora com a criação das políticas e revisão de contratos (cláusula LGPD);

Recursos Humanos – Dissemina a cultura da privacidade/proteção de dados por meio de treinamento e capacitação da equipe; Promove a conscientização e o treinamento;

Auditoria – Realiza inventário, mapeamento, análise do risco de vazamento, vulnerabilidades e análises periódicas do tratamento de dados pessoais;

Tecnologia da Informação – Investimento em tecnologia é uma das medidas e ações recomendadas para que seja viável o melhor controle de acesso aos dados pessoais, segurança dos dados armazenados, segurança das comunicações, bem como dos dados pessoais sensíveis que fazem parte da área médica;

Fornecedores – Adequação contratual estabelecendo direitos e obrigações quanto ao tratamento de dados pessoais e, principalmente, às responsabilidades dos controlados e operadores. Devem prever cláusula de proibição de desvio de finalidade sem autorização e regras específicas para acessos à base de dados.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

DOCUMENTOS SUGERIDOS PARA IMPLANTAÇÃO DA LGPD

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

I. TERMO DE CONSENTIMENTO

Para a atividade do médico, em seu consultório, sugere-se a elaboração de termos de consentimento para o tratamento de dados pessoais de pacientes, visitantes/familiares, funcionários e prestadores de serviço. O médico já está familiarizado com esse tipo de documento e ainda existem outros semelhantes, como os para transfusão de sangue, exames diagnósticos e termo de ciência e consentimento informado para a realização de procedimentos cirúrgicos e invasivos.

Caso o atendimento seja realizado de maneira virtual, deverá seguir as normas da Telemedicina (Resolução CFM 2314/2022) e do Marco Civil da Internet (Lei 12.965/2014). A prestação de serviço de saúde com padrões digitais deverá seguir os padrões normativos e éticos usuais do atendimento presencial, com o custeio da empresa e formas de remuneração possíveis ao seu tempo.

Os termos de consentimento devem conter informações específicas para cada paciente, sendo essencial os dados pessoais do paciente (que o identifiquem), os do profissional médico que atende aquele paciente, as cláusulas de tratamento de dados pessoais e os direitos do titular/paciente, bem como cláusula em caso de vazamento de dados.

Importante salientar que os termos de consentimento para o tratamento de dados de crianças e adolescentes devem ser diferenciados, específicos e em destaque, pois devem ser assinados pelos responsáveis legais (ao menos um). A própria LGPD estabelece as diretrizes em seu artigo 14. A linguagem deve ser clara e acessível, de maneira simples para o adequado entendimento.

Ao elaborar um Termo de Consentimento, o consultório deverá:

- Inserir a especificação e o propósito de se coletarem esses dados;
- Informar se os dados serão compartilhados com terceiros (laboratórios, telemedicina, telerradiologia etc);
- Apontar os contatos dos responsáveis pela proteção de dados ou do *Data Protection Officer* (DPO), para o caso de esclarecimento de dúvidas.

2. TERMO DE CONFIDENCIALIDADE/SIGILO (COLABORADORES, PRESTADORES, TERCEIROS)

O termo de sigilo, compromisso e confidencialidade deverá ser elaborado visando o cumprimento da LGPD também pelos funcionários, colaboradores, prestadores de serviço e terceiros envolvidos na atividade do médico. Importante que constem as cláusulas de responsabilidade, do acesso às informações sigilosas, aos dados pessoais e dados pessoais sensíveis, bem como das obrigações e penalidades aplicadas e do objeto do contrato.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Segundo a ANPD: *"Essa política pode ser endereçada por organizações de qualquer porte e compreende uma boa prática para a gestão da segurança. Muito embora não seja obrigatória, a elaboração dessa política e sua implementação são incentivadas pela ANPD aos agentes de tratamento de pequeno porte porque evidenciam boa-fé e diligência na segurança dos*

dados pessoais sob sua custódia e fornecem as diretrizes para a gestão da segurança da informação.O propósito fundamental da PSI é ser uma ferramenta que apoie a implementação de um processo estruturado de segurança da informação adequado a cada organização, considerando seu negócio e seu porte.[5]"

SEGURANÇA, PROTEÇÃO E GUARDA DOS DADOS

Iniciativas para aprimorar a segurança e proteção dos dados pessoais:

I. CONTROLE DE ACESSO

- Implementar um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais;
- Configurar funcionalidades no sistema de controle de acesso que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade;
- Implementar um adequado gerenciamento de senhas, estabelecendo controles, tais como:
  - Evitar o uso de senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos;
  - Utilizar apenas senhas complexas para acessar aplicativos e outros sistemas informáticos;
  - Não reutilizar senhas;
  - Proibir o compartilhamento de contas ou de senhas entre funcionários. Aplicar o princípio do menor privilégio (*need to know*);

[5] Publicação Segurança da Informação para Agentes de Tratamento de Pequeno Porte, da ANPD

Utilizar a autenticação multifator para acessar sistemas ou base de dados que contenham dados pessoais.

- Implementar um sistema de controle de acesso aplicável a todos os usuários que acessam o sistema de TI (caso o agente de tratamento possua rede interna de computadores).

2. SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados;

- Implementar soluções de pseudonimização, como a criptografia, para cifrar dados pessoais;
- Orientar os funcionários para não desativar ou ignorar as configurações de segurança de estações de trabalho;
- Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos;
- Inventariar e cifrar dados de dispositivos externos e armazená-los em locais seguros;
- Realizar *backups offline*, periódicos e armazená-los de forma segura;
- Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá- las ou, quando não for possível a sobrescrita, destruir as mídias físicas;

- Estabelecer no contrato de serviço o registro da destruição/descarte (caso o agente de tratamento utilize serviços de terceiros para o descarte).

3. SEGURANÇA DAS COMUNICAÇÕES

- Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia "fim a fim", para serviços de comunicação;
- Instalar e manter um sistema de *firewall* e/ou utilizar um *Web Application Firewall* (*WAF* – Filtro de Aplicação);
- Proteger emails via adoção de ferramentas AntiSpam, filtros de email e integrar o antivírus ao sistema de email;
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.

4. GERENCIAMENTO DE VULNERABILIDADES

- Atualizar periodicamente todos os sistemas e aplicativos utilizados, mantendo-os em sua versão atualizada (instalar patches de segurança disponibilizados pelos fornecedores);
- Adotar e atualizar periodicamente softwares antivírus e antimalwares. Realizar varreduras antivírus periódicas nos dispositivos e sistemas utilizados.

5. DISPOSITIVOS MÓVEIS

- Utilizar técnicas de autenticação multifator para controle de acesso de dispositivos móveis – como smartphones e laptops;

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

- Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível;
- Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

6. SERVIÇOS EM NUVEM

- Realizar um contrato, de acordo com o nível de serviço com o provedor de serviços em nuvem, contemplando a segurança dos dados armazenados;
- Avaliar se o serviço oferecido pelo provedor do serviço em nuvem atende aos demais requisitos de segurança da informação estabelecidos;
- Analisar os requisitos para o acesso do usuário a cada serviço em nuvem utilizado;
- Utilizar técnicas de autenticação multifator para acesso aos serviços em nuvem relacionados a dados pessoais.

O QUE FAZER EM CASOS DE INCIDENTES DE SEGURANÇA

Em caso de acesso não autorizado, divulgação, alteração ou perda de dados pessoais, seja de forma acidental como de forma ilícita, a LGPD determina que os agentes de tratamento adotem as seguintes medidas imediatas:

- Avaliação interna do incidente;
- Comunicação do incidente ao controlador;
- Comunicação pelo encarregado à ANPD;

- Notificação do incidente aos titulares;
- Elaboração de documento de avaliação do incidente e adoção de medidas de segurança.

ENCARREGADO DE DADOS

Como vimos anteriormente, o consultório deverá nomear um encarregado de proteção de dados, uma nova função que surge com a LGPD, conhecido também como *Data Protection Officer* (DPO).

Em síntese, o DPO de um consultório é aquela pessoa física ou jurídica responsável por assegurar a execução da política interna de tratamento de dados. Isso significa verificar que os procedimentos dentro do consultório estejam sendo executados e seguidos de acordo com a LGPD, tanto por médicos quanto por enfermeiros, auxiliares, secretárias e demais profissionais contratados, inclusive terceirizados.

A recomendação é que a posição de DPO dentro de um consultório seja preenchida por um profissional que reúna habilidades de comunicação e conhecimentos multidisciplinares, incluindo a LGPD. Isso porque o DPO deverá aceitar reclamações e se comunicar com o paciente a respeito dos seus dados pessoais, quando preciso, e também com a Autoridade Nacional de Proteção de Dados (ANPD).

V – CONSEQUÊNCIAS NO DESCUMPRIMENTO DA LGPD

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

A LGPD contemplou dois sistemas voltados à execução de suas normas, disciplinando regras específicas para a responsabilização dos agentes de tratamento (controlador e operador): um cível-jurisdicional e outro administrativo-sancionador.

O primeiro sistema consiste, principalmente, no reconhecimento do **dever de indenizar** os **danos patrimoniais, morais, individuais** ou **coletivos** causados em razão do descumprimento da legislação de proteção de dados pessoais (Artigo 42). Portanto, é possível afirmar que a desobediência à LGPD caracteriza um **ato ilícito**, sendo precursora da **responsabilidade civil**. O valor da indenização irá corresponder à "extensão do dano" (Artigo 944 do Código Civil). Naturalmente, há um certo grau de complexidade na delimitação dos danos morais, sendo certo que a LGPD não estabeleceu parâmetros objetivos para este arbitramento.

De modo inovador, foi determinada a **responsabilidade solidária entre o operador e o controlador de dados**, bem como entre **todos os controladores**, quando presente uma das hipóteses do Artigo 42, § 1º:

Artigo 42, § 1º A fim de assegurar a efetiva indenização ao titular dos dados:

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

> I - *o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no Artigo 43 desta Lei;*
> II - *os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no Artigo 43 desta Lei.*

Nesses casos, o titular lesado poderá exigir a totalidade da indenização do operador, do(s) controlador(es) ou de todos, conjuntamente.

Com o mesmo intento de facilitar a tutela dos direitos lesados, a LGPD autorizou os juízes a inverterem o ônus da prova nos processos indenizatórios movidos pelo lesado. Em termos práticos, caberá ao agente de tratamento de dados demonstrar que atuou com diligência, bem como a ausência de violação da legislação.

Foram fixadas três hipóteses excludentes da responsabilidade civil (Artigo 43):

EXCLUDENTES DA RESPONSABILIDADE CIVIL

Controlador/ Operador demonstrar que não realizou o tratamento de dados pessoais	Controlador/ Operador provar que não houve violação à legislação de proteção de dados	Controlador/ Operador comprovar que o dano decorreu exclusivamente da culpa do titular dos dados ou de terceiro

Em suma, constatada a violação à LGPD, o titular dos dados poderá ajuizar uma ação judicial cível contra os agentes de tratamento, pleiteando a reparação dos danos sofridos.

REQUISITOS DA RESPONSABILIDADE CIVIL

CONDUTA

Ação ou omissão praticada no exercício de atividade de tratamento de dados pessoais, com violação da legislação de proteção de dados pessoais (Artigo 42). Tratamento de dados pessoais com a inobservância da legislação ou sem o fornecimento da segurança que o titular pode esperar.

DANO

Lesão patrimonial ou moral.
Dano individual ou coletivo.

NEXO CAUSAL

Relação de causalidade entre a conduta e o dano.

CULPA

Imperícia, imprudência ou negligência.
Abuso de direito. Dolo.

Se os dados pessoais vazados forem sensíveis – a exemplo de informações relacionadas à saúde do paciente (Artigo 5º, inc. II, da LGPD) –, aumenta-se significativamente a probabilidade do reconhecimento de dano indenizável, ainda que apenas moral (AC 1000331-24.2021.8.26.0003, Rel. Des. Alfredo Attié, TJSP – 27ª Câmara de Direito Privado, DJe 16/11/2021).

Ao lado da responsabilização civil, a infração às normas da LGPD poderá ensejar condenações administrativas dos agentes de tratamento de dados. Nesses casos, caberá à Autoridade Nacional de Proteção de Dados (ANPD) fixar as penas apropriadas, dentre aquelas previstas no Artigo 52 da LGPD.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

ADVERTÊNCIA

Fixação de prazo para a adoção de medidas corretivas.

Até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado.

Limite de R$ 50 milhões por infração.

MULTA DIÁRIA

Observados os limites da multa simples.

PUBLICIZAÇÃO DA INFRAÇÃO

Após a confirmação da ocorrência da violação à LGPD.

BLOQUEIO DOS DADOS PESSOAIS RELACIONADOS À INFRAÇÃO

Poderá perdurar até a regularização da situação.

ELIMINAÇÃO DOS DADOS PESSOAIS

Os dados a serem eliminados devem estar relacionados à infração verificada.

SUSPENSÃO PARCIAL DO FUNCIONAMENTO DO BANCO DE DADOS

Poderá perdurar pelo prazo máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento de dados.

SUSPENSÃO DO EXERCÍCIO DA ATIVIDADE DE TRATAMENTO DOS DADOS PESSOAIS

Poderá perdurar pelo período máximo de 6 meses, prorrogável por igual período.

PROIBIÇÃO PARCIAL OU TOTAL DO EXERCÍCIO DE ATIVIDADES

As atividades proibidas devem estar relacionadas ao tratamento de dados.

ESPECIFICIDADES DA SANÇÃO ADMINISTRATIVA

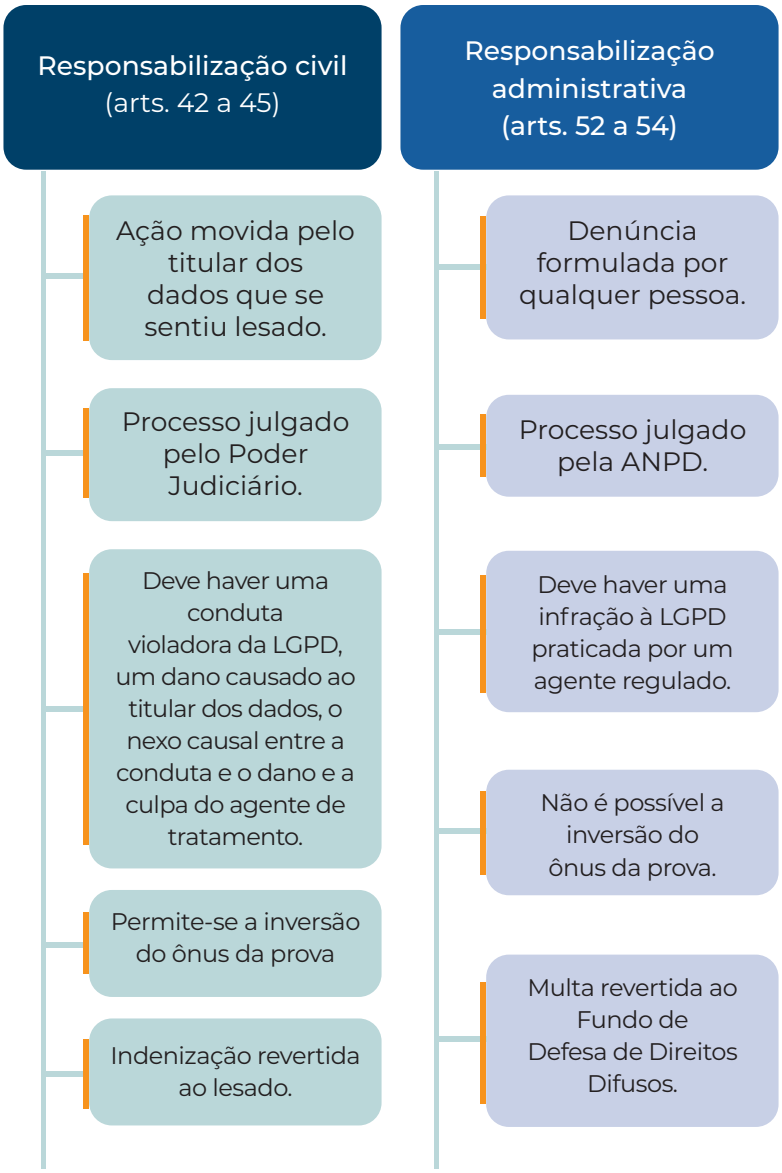
As sanções somente poderão ser aplicadas após procedimento administrativo no qual deverá ser garantida a ampla defesa.

As sanções poderão ser aplicadas de forma isolada ou cumulativa.

A gradação das sanções deverá observar os seguintes critérios:

1. Gravidade e natureza das infrações e dos direitos pessoais afetados;
2. Boa-fé do infrator;
3. Vantagem auferida ou pretendida pelo infrator;
4. Condição econômica do infrator;
5. Reincidência;
6. Grau do dano;
7. Cooperação do infrator;
8. Adoção de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
9. Adoção de política de boas práticas e governança;
10. Pronta adoção de medidas corretivas;
11. Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Vale ressaltar que a aplicação de penas pela ANPD não afasta a responsabilização civil ou penal daquele que violar a LGPD; tampouco inviabiliza outras condenações administrativas por entidades competentes (Artigo 52, § 2º). Dessa forma, uma única violação[6] à LGPD poderá ensejar diversas condenações administrativas e jurisdicionais.



[6] Por exemplo, o médico responsável técnico de um consultório que, por negligência, contribui para o vazamento de dados sensíveis dos pacientes poderá ser condenado judicialmente a reparar os danos causados aos titulares dos dados, penalizado pela ANPD, além de punido pelo Conselho Regional de Medicina competente por transgredir a ética profissional.

VI – NORMAS RELACIONADAS

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

TELEMEDICINA – Resolução CFM nº 2.314, de 20/04/2022 - Define e regulamenta a telemedicina, como forma de serviços médicos mediados por tecnologias de comunicação.

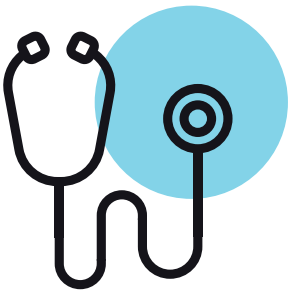
CERTIFICAÇÃO DIGITAL - Resolução CFM nº 2.296, de 05/08/21 – Regulamenta o Sistema Integrado de Identificação Médica (SIIM), disciplinando e normatizando a emissão de documentos de identificação médica físicos e digitais;

Circular do CFM Nº SEI-303/2022/CFM/SEGED, de 27/09/22 - Amplia a validação dos Certificados de Especialidade AMB para o registro da(s) especialidade(s) nos Conselhos de Medicina.

PRONTUÁRIO MÉDICO - Resolução CFM nº 1.638, de 09/08/2002 - Define prontuário médico e torna obrigatória a criação da Comissão de Prontuário nas instituições de saúde.

PRONTUÁRIO MÉDICO ELETRÔNICO - Resolução CFM nº 2.299, de 26/10/2021 - Regulamenta, disciplina e normatiza a emissão de documentos médicos eletrônicos.

Resolução CFM nº 2.218, de 29/11/2018 - Revoga o artigo 10º da Resolução CFM nº 1.821/2007, de 23 de novembro de 2007, que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em Saúde.



VII – PERGUNTAS E RESPOSTAS

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

DEVO ENTREGAR O PRONTUÁRIO MÉDICO PARA UM DELEGADO DE POLÍCIA?

Os delegados de polícia não podem requisitar diretamente aos hospitais e/ou médicos os prontuários médicos e/ou fichas médicas dos seus pacientes por estar esta requisição vinculada à cláusula de reserva de jurisdição, por se tratar de quebra do sigilo de documento potencialmente portador de fatos relativos à privacidade e à intimidade da pessoa humana. DESPACHO CFM COJUR Nº 129/14. https://shre.ink/kn2g

QUANDO É PERMITIDO COLOCAR CID EM ATESTADO MÉDICO?

De acordo com o artigo 5º da Resolução CFM nº 1.658, de 13/12/2002, https://shre.ink/knkW:

> *"Os médicos somente podem fornecer atestado com o diagnóstico codificado ou não quando por justa causa, exercício de dever legal, solicitação do próprio paciente ou de seu representante legal.*
> ***Parágrafo único:** No caso da solicitação de colocação de diagnóstico, codificado ou não, ser feita pelo próprio paciente ou seu representante legal, esta concordância deverá estar expressa no atestado".*

COMO REALIZAR CORRETAMENTE A PRESCRIÇÃO MÉDICA AO PACIENTE?

Conforme apontado na Resolução CREMESP nº 278, de 23/09/2015. https://shre.ink/knkq, que regulamenta a prescrição médica de medicamentos no âmbito do Estado de São Paulo: *"Artigo 4º - O médico deve entregar ao paciente a prescrição em quantas vias forem necessárias à dispensação do respectivo medicamento.*

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Artigo 5º – A identificação da doença na prescrição, ainda que pelo CID, somente pode ser feita com autorização expressa do paciente.

Artigo 6º – O médico deverá incluir na receita médica, o endereço residencial do paciente, para fins de utilização no âmbito do Programa Farmácia Popular do Brasil".

O MÉDICO DEVE FORNECER RELATÓRIO MÉDICO QUANDO SOLICITADO PELO PACIENTE?

"O paciente tem direito a ter atestada sua condição física, devendo o médico limitar-se a declarar somente o fato efetivamente constatado". - Consulta nº 4.337/02. https://shre.ink/knGG

"A elaboração do relatório médico é antes de tudo uma obrigação ética, e não cabe obviamente nenhum tipo de cobrança." - Consulta nº 48.735/00. https://shre.ink/knGx

QUAL DESTINO DEVE SER DADO AOS PRONTUÁRIOS DE MÉDICO FALECIDO?

Os prontuários médicos elaborados em fichas impressas e cujo último registro tenha sido lançado há mais de 20 anos podem ser incinerados. Já os prontuários impressos, com registros de atendimentos com menos de 20 anos, devem ser preservados ou as informações informatizadas (meio óptico, microfilmado ou digitalizado), com nível de segurança 2 (NGS2), antes de serem incinerados, conforme Consulta 101.346/14. https://shre.ink/knn0

QUAL O DESTINO DOS PRONTUÁRIOS MÉDICOS NO CASO DE FECHAMENTO OU ENCERRAMENTO DE ATIVIDADES?

A Resolução CFM ° 1.821/07 estabelece que todo o arquivo deve ser mantido por 20 anos, sob a responsabilidade do profissional ou do estabelecimento de saúde, contados da data

do último registro. No entanto, apesar de se tratar de material que não pode ser descartado, por conta do sigilo, essa condição pode gerar empecilhos para a família do profissional quando este falece, ao próprio médico quando decide encerrar suas atividades e aos hospitais quando do seu fechamento.

A respeito do tema, o CFM emitiu o Processo Consulta nº 3.120/94-CFM (31/95) https://shre.ink/knnK:

"Quando o arquivo pertencer a uma instituição, hospital ou casa de saúde, um substituto ocupará a sua função e herdará os arquivos, pois, conforme já dito, o arquivo pertence ao local de trabalho.

Podem também ser considerados herdeiros, mesmo em consultórios, serviços e departamentos particulares, os médicos assistentes diretos, com os quais a própria clientela detinha o costume e a indicação da confiança do titular, quando em exercício."

Conforme a Consulta Cremesp nº 118.721/18 https://shre.ink/kn1i, *"quando há uma sucessão empresarial ou profissional, os documentos médicos devem ser simplesmente transferidos aos novos profissionais ou aos que permanecerem na instituição, até pelo fato de que há a probabilidade dos pacientes procurarem o serviço novamente, mesmo que sob outra denominação empresarial ou novo corpo clínico"*.

E quando há um profissional, sem que seja possível definir o que o CFM convencionou chamar de "herdeiro médico", também há posicionamento no referido parecer:

"Com a morte se esvai toda a responsabilidade do médico pelo segredo. O que deveria ter sido informado aos pacientes ou responsáveis, ou notificado compulsoriamente, com certeza já fora feito em vida ou, pelo seu entendimento em contrário quanto a casos específicos, deve acompanhá-lo ao sepulcro. É óbvio que não podem ser os

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

familiares responsáveis naturais ou ***ad hoc*** *pela guarda dos arquivos, por determinação de normas ou leis sanitárias, ético-profissionais ou da Justiça comum. Na verdade, assim deve ser, não somente pela responsabilidade jurídica, mas também por que somente caberia ao médico já falecido definir o que poderia ser ou deixar de ser a violação do lacre do bom senso para o acesso à informação.*

Tendo em vista o exposto, o arquivo particular de médico falecido sem herdeiro profissional deve então ser incinerado por pessoa de convivência diária direta, familiares ou secretária particular".

Quando o médico se aposenta, abandona a profissão ou encerra suas atividades na Medicina, sem ninguém que o suceda, não há motivo para que ele permaneça por mais 20 anos mantendo um arquivo de forma onerosa, sem que possa, em definitivo, encerrar seu exercício profissional.

Nestes casos, o parecer do Cremesp — Consulta nº 118.721/18 https://shre.ink/kn1i — recomenda que deva ser adotada a mesma sistemática indicada quando do óbito. *"O encerramento particular das atividades finaliza sua vida profissional, fazendo com que o médico se desligue de seus pacientes."*. Mas ressalva que, *"antes de mandar incinerar, o profissional deve publicar um pequeno Edital, em jornal de circulação em sua área de atuação, informando o encerramento das atividades e que, a partir de uma data pré-definida, irá incinerar a documentação médica sob sua responsabilidade. Desta forma, os pacientes que tiverem interesse em retirar sua documentação, poderão procurá-lo para assim proceder. Tal medida, além de indicar uma responsabilidade do profissional, torna transparente e facilita o acesso de seus antigos pacientes à informação".*

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

O tema também é abordado na Consulta Cremesp nº 101.806/13 https://shre.ink/kn1W

O PACIENTE TEM DIREITO AO ACESSO E OBTER CÓPIA DE SEU PRONTUÁRIO?

De acordo com o Código de Ética Médica (Resolução CFM nº 2.217/2018) https://shre.ink/kFBu, no Capítulo X – Documentos Médicos:

– É vedado ao médico:

"Artigo 88 :

- Negar ao paciente ou, na sua impossibilidade, a seu representante legal, acesso a seu prontuário, deixar de lhe fornecer cópia quando solicitada, bem como deixar de lhe dar explicações necessárias à sua compreensão, salvo quando ocasionarem riscos ao próprio paciente ou a terceiros."

O MÉDICO PODE UTILIZAR-SE DO PRONTUÁRIO MÉDICO DE PACIENTE PARA DEFESA EM JUÍZO?

"Para sua defesa judicial, o médico poderá apresentar a ficha ou prontuário médico à autoridade competente, solicitando que a matéria seja mantida em segredo de Justiça", como indica o Artigo 7º da Resolução CFM 1.605/2002. https://shre.ink/knzD

O MÉDICO AUDITOR PODE TER ACESSO AO PRONTUÁRIO MÉDICO DE DETERMINADO PACIENTE, A PEDIDO DA OPERADORA DE SAÚDE?

A Resolução CFM 1.614/2001. https://shre.ink/knAO diz, em seu artigo 7º: *"O médico, na função de auditor, tem o direito de acessar, in loco, toda a documentação necessária, sendo-lhe vedada a retirada dos prontuários ou cópias da instituição, podendo, se necessário, examinar o paciente, desde que devidamente autorizado pelo mesmo, quando possível, ou por seu representante legal"*.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

COMO ARMAZENAR DADOS DO PACIENTE EM PRONTUÁRIO DIGITAL? PODE-SE DIGITALIZAR OS PRONTUÁRIOS? QUANTO TEMPO DEVE O MÉDICO GUARDÁ-LO?

A Resolução CFM 1.821/2018. https://shre.ink/knAh estabelece que o armazenamento deve ser feito da seguinte maneira:

"Artigo 1º – Aprovar o Manual de Certificação para Sistemas de Registro Eletrônico em Saúde, versão 3.0 e/ou outra versão aprovada pelo Conselho Federal de Medicina, anexo e também disponível nos sites do Conselho Federal de Medicina e Sociedade Brasileira de Informática em Saúde (SBIS), respectivamente, www.portalmedico.org.br e www.sbis.org.br.

Artigo 2º – Autorizar a digitalização dos prontuários dos pacientes, desde que o modo de armazenamento dos documentos digitalizados obedeça a norma específica de digitalização contida nos parágrafos abaixo e, após análise obrigatória da Comissão de Revisão de Prontuários, as normas da Comissão Permanente de Avaliação de Documentos da unidade médico-hospitalar geradora do arquivo.

§ 1º – Os métodos de digitalização devem reproduzir todas as informações dos documentos originais.

Artigo 8º – Estabelecer o prazo mínimo de 20 (vinte) anos, a partir do último registro, para a preservação dos prontuários dos pacientes em suporte de papel, que não foram arquivados eletronicamente em meio óptico, microfilmado ou digitalizado."

HÁ NECESSIDADE DE INCLUIR CPF OU CNPJ NA PRESCRIÇÃO MÉDICA?

Quando houver previsão em lei acerca da necessidade de se incluir o CPF ou CNPJ do emitente na receita, esta deve ser obedecida, em atenção ao Princípio da Legalidade, de acordo com o Despacho CFM Cojur nº 237/2019. https://shre.ink/knAb

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

COMO OBTER A ASSINATURA ELETRÔNICA PARA PRESCRIÇÃO DIGITAL?

Para orientações a respeito, acesse:
https://prescricaoeletronica.cfm.org.br

O COMPARTILHAMENTO DE DADOS VIA APLICATIVOS, COMO WHATSAPP, ESTÁ EM CONFORMIDADE COM A LGPD?

Uma mensagem com dados clínicos sensíveis de um paciente, enviada equivocadamente a terceiros, sem prévia autorização ou meios de proteção, é ilegal. Nos casos, por exemplo, de clonagem de contas de WhatsApp, um eventual vazamento também é de responsabilidade do médico, pois é considerado controlador de dados, o que resulta na responsabilidade legal por eventuais falhas de segurança e no risco de penalidades.

O uso do aplicativo Whatsapp pelos médicos diante do compartilhamento de informações e dados foi alvo do:

* Parecer Cremesp nº 17.574/21
https://shre.ink/knIV

- Parecer CFM nº 24/16 https://shre.ink/knIL

- Processo Consulta CFM nº 14/2017
https://shre.ink/knIe

- Despacho Sejur CFM nº 373/2016
https://shre.ink/knIr

REFERÊNCIAS:

- Lei Geral de Proteção de Dados – 13.709/18
- Cartilha CFM LGPD – A Lei Geral de Proteção de Dados Pessoais e atuação do profissional da Medicina – 2022
- Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf
- Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD) https://www.gov.br/governo-digital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf
- Guia Orientativo de Segurança da Informação direcionado aos agentes de tratamento de pequeno porte https://shre.ink/kncO
- LGPD na Saúde – Analluza Bolivar Dallari e Gustavo Ferraz de Campos Monaco – Revista dos Tribunais – ISBN – 978-65-5614-955-4
- LGPD Para Consultórios | Área da Saúde | OAB-SP – Novembro/2021 – Comissão Especial de Privacidade e Proteção de Dados Pessoais – GT Privacidade na Saúde https://shre.ink/kncA
- Código de Boas Práticas – Proteção de Dados para Prestadores Privados em Saúde – Confederação Nacional de Saúde https://shre.ink/kniE
- Cartilha de Proteção de Dados Pessoais no Setor da Saúde https://shre.ink/kniC - Opice Blum, Bruno e Vainzof Advogados Associados.

Índice
INTRODUÇÃO
I
II
III
IV
V
VI
VII

GUIA LGPD CREMESP

COMENTADO EDIÇÃO 2023

CREMESP

CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO